Safeonweb.be

ONLINEBETRÜGEREIEN:

WIE KANN MAN SIE ERKENNEN,
WIE KANN MAN SIE VORBEUGEN
UND WIE SOLL MAN REAGIEREN ?

Weitere Informationen und andere Formen des Betrugs sind auf safeonweb.be/de verfübar

CENTRE FOR CYBERSECURITY BELGIUM

.be

Phishing

Phishing ist Online-Betrug durch gefälschte E-Mails, Websites, SMS, QR-Codes, usw. Das Ziel besteht darin, Ihre persönlichen Informationen zu sammeln.

- Denken Sie nach, bevor Sie klicken, denn Angebote können trügerisch sein.
- Geben Sie niemals Passwörter, Bankkarten-PINs oder Digipass-Antwortcodes per E-Mail, Telefon, SMS oder über soziale Netzwerke weiter.
- Überprüfen Sie die Absenderadresse und die URL der Links, zu denen Sie geschickt werden.
- Lernen Sie auf surfenohnerisiko.safeonweb.be, wie Sie verdächtige Nachrichten erkennen können.

Anlagebetrug

Sie erhalten einen Anruf oder werden per E-Mail (oder über den gehackten Account eines Freundes) durch eine vorgebliche Investitionsgesellschaft kontaktiert, die Ihnen anbietet Aktien oder andere Finanzprodukte zu kaufen. Es kann sich auch um eine falsche Werbung handeln, in der ein Prominenter diese Investitionen anpreist.

- Hüten Sie sich vor finanziellen Angeboten, um die Sie nicht gebeten haben, und bleiben Sie besonders kritisch.
- Überprüfen Sie die Identität des Dienstleisters, auch wenn es sich um ein zugelassenes Unternehmen zu handeln scheint: Name, Gesellschaftssitz, Kontaktdaten.

PC-Problem (Tech Scam)

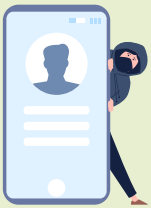
- Seien Sie misstrauisch bei Telefonanrufen von Unternehmen, die Sie auffordern, eine Reihe von Aktionen auf Ihrem Computer durchzuführen.
- Wenn ein Popup-Fenster erscheint, in dem Ihnen mitgeteilt wird, dass Ihr Computer gesperrt ist, wenden Sie sich nicht an die angegebene Nummer. Führen Sie einen Antiviren-Scan durch.
- Installieren Sie niemals eine Anwendung oder Software, die von dem angeblichen Helpdesk angeboten wird. Dadurch könnte dieser die Kontrolle über Ihr Gerät übernehmen.

Identitätsdiebstahl/gehacktes Konto

> Mit meinem Konto passieren merkwürdige Dinge: Ich habe angeblich Nachrichten an meine Freunde geschickt, ohne es zu wissen, und auf meiner Seite erscheinen Nachrichten und Fotos, die ich nicht selbst gepostet habe.

Ihr Konto wurde wahrscheinlich gehackt.

- Haben Sie noch immer Zugang zu Ihrem Konto? Ändern Sie sofort das Passwort dieses Kontos und Ihrer anderen Konten, und benachrichtigen Sie Ihre Kontakte.
- Haben Sie keinen Zugang mehr? Verwenden Sie die Wiederherstellungsoptionen (Option „Passwort vergessen“), um wieder Zugang zu erhalten und ändern Sie danach alle Ihre Passwörter.
- Aktivieren Sie die Zwei-Faktor-Authentisierung bzw. Bestätigung in zwei Schritten. Im ersten Schritt melden Sie sich mit Ihrem Kennwort bei Ihrem Konto an. Im zweiten Schritt sendet dieses Konto z. B. einen Code an Ihr Handy, den Sie eingeben um Zugang zu Ihrem Konto zu erhalten.
- Verwenden Sie für jedes Konto ein anderes (starkes) Passwort und bewahren Sie diese Passwörter in einem Kennwort- bzw. Passwortmanager auf. Es handelt sich um einen Online-Safe, in dem Ihre Passwörter für jeden Account verwahrt werden. Der Safe selbst ist ebenfalls mit einem Passwort geschützt.



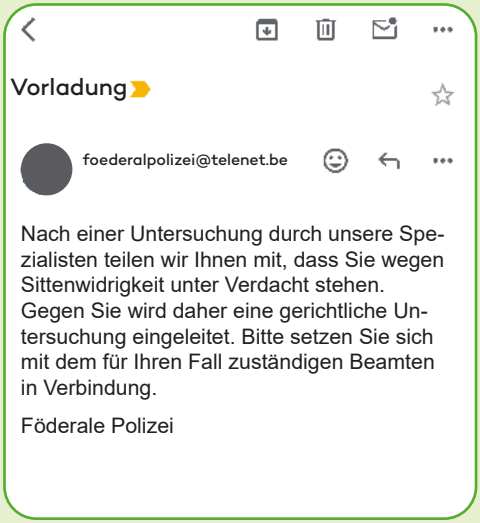
Betrug im Online-Handel

Dieser Betrug zielt auf den Käufer oder den Verkäufer auf Online-Verkaufsplattformen ab. Dabei kann es sich um falsche Käufer oder falsche Verkäufer, oder auch um falsche Websites handeln.

Hallo, ist dieser Artikel noch verfügbar? Ich biete Ihnen 500 € für Ihren Tisch. Ich kann ihn nicht abholen, also wird er von einem DPD-Fahrer abgeholt. Ich werde Ihnen den Betrag überweisen.

- Hüten Sie sich vor zu schnellen Antworten und Angeboten, die über dem geforderten Preis liegen. Überprüfen Sie das Profil des Käufers/Verkäufers.
- Führen Sie Ihre Gespräche mit den Käufern/Verkäufern immer auf der Online-Verkaufsseite fort und wechseln Sie nicht z. B. zu SMS oder WhatsApp.
- Bezahlen Sie niemals über einen Link, der Ihnen von einem Käufer oder Verkäufer zugesandt wurde. Diese Links führen Sie zu einer gefälschten Website, auf der die Betrüger Ihre Bankdaten abfragen.
- Geben Sie niemals Ihre persönlichen Daten auf der Website eines Transportunternehmens über einen Link ein, den Ihnen der Käufer/Verkäufer geschickt hat.

Nachricht, die scheinbar von der Polizei stammt



Hier geht es um E-Mail-Betrug, der auf die Dringlichkeit und Schwere der Vorwürfe setzt.

- Reagieren Sie niemals auf eine solche Nachricht und gehen Sie nicht auf Geldforderungen ein.
- Blockieren Sie den Absender.
- Kontaktieren Sie die Stelle, von der die Nachricht gesendet wurde, über die Kontaktdaten, die Sie selbst recherchiert haben.

Meine Checklist zur Online-Sicherheit

- ✅ Ich gebe niemals Passwörter, PINs oder Antwortcodes per E-Mail, Telefon, SMS oder über soziale Netzwerke weiter.
- ✅ Ich schütze meine Mailbox und meine Accounts auf sozialen Netzwerken mit der Zwei-Faktor-Authentisierung.
- ✅ Ich installiere Updates, sobald sie verfügbar sind.
- ✅ Ich installiere ein Antivirenprogramm auf meinem Computer, sollte ich das noch nicht haben.
- ✅ Ich erstelle Sicherungskopien meiner Dateien in der Cloud oder auf einer externen Festplatte.

Zu spät – Sie sind zum Opfer geworden. Was können Sie jetzt tun?

Sie haben Ihre Bankdaten übermittelt, Sie stellen betrügerische Geldabbuchungen von Ihrem Konto fest oder Sie haben Geld an einen Betrüger überwiesen?

- Wenden Sie sich an Card Stop unter 078 170 170, um den Zugriff auf Ihre Konten zu sperren.
- Kontaktieren Sie Ihre Bank. Je früher Sie sie benachrichtigen, desto höher sind Ihre Chancen, das Geld zurückzubekommen.
- Erstatten Sie bei der örtlichen Polizei Anzeige. Halten Sie so viele Informationen wie möglich bereit: Kontoauszüge, Screenshots der betrügerischen Nachricht oder Website, des Profils und der Gespräche mit der verdächtigen Person, der installierten Anwendung usw.

DIE TOOLS UM SIE ZU SCHÜTZEN

SIE HABEN EINE VERDÄCHTIGE E-MAIL ODER NACHRICHT ERHALTEN?

Senden Sie sie an die Adresse suspekt@safeonweb.be und löschen Sie sie anschließend. Verdächtige Anhänge und Links werden automatisch analysiert. Wenn ein weniger aufmerksamer Internetnutzer später auf denselben Link klickt , erhält er eine deutliche Warnung, diese Seite nicht zu besuchen.

INSTALLIEREN SIE DIE SAFEONWEB BROWSER-ERWEITERUNG

Die Safeonweb Browser-Erweiterung warnt Sie, wenn Sie eine unsichere Website besuchen und es gefährlich ist Ihre Daten einzugeben. Ein Farbcode (sichtbar in der Symbolleiste) zeigt Ihnen an, ob die Website vertrauenswürdig ist oder nicht. Sehen Sie sich auf safeonweb.be an, wie Sie die Erweiterung installieren können.

SEHEN SIE SICH UNSERE E-LEARNING-SERIE „SURFEN OHNE RISIKO“ AN

Lernen Sie mit unserer E-Learning-Serie auf surfenohnerisiko.safeonweb.be, wie Sie Betrügereien und verdächtige Nachrichten erkennen können.

LADEN SIE DIE SAFEONWEB-APP HERUNTER

Die Safeonweb-App informiert Sie über die aktuellen Bedrohungen im Land und gibt Ihnen Tipps, wie Sie Ihre Online-Sicherheit verbessern können.
Sie ist kostenlos für iOS im App Store und für Android im Google Play Store erhältlich.

WEITERE INFOS?

- **safeonweb.be/de**
- **surfenohnerisiko.safeonweb.be/de/modules**

Folgen Sie Safeonweb auf